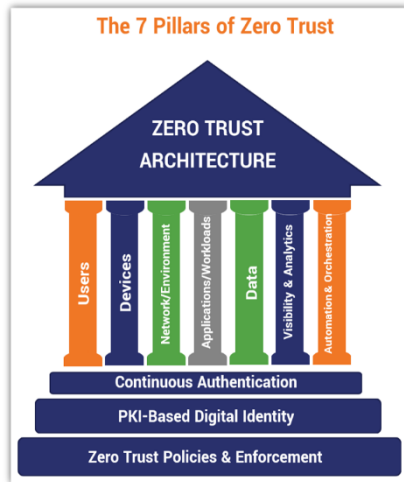# CIO Strategic Guidance Initiatives

Zero Trust Implementation

What: Zero Trust assumes that your environment (network/devices) is compromised at all times and focuses on standards to reduce (never eliminate) impact to data, information, and operations.

How: Introduces standards and best practices at all layers of the OSI Model. These standards and best practices are not all technology-based but can also be least privilege and other best practices that control technology to reduce our footprint, attack surface and vulnerabilities.

Why: Zero Trust Implementation is becoming the industry standard for organizations to protect data, network, mobile, infrastructure, endpoint, and cloud architectures.

Who: PMO, EA, Digital Government, Security, Administrative, Governance and Leadership Teams

Related Efforts:

1. Innovate Technologies Initiative
2. Agency Segmentation/VLAN Implementation
3. Encryption/PKI Implementation
4. End of Life & Unsecure Service Removal
5. Proxy Implementation
6. MPLS Cloud & Redundant Access Implementation
7. VDI Implementation
8. Log Storage Expansion

Data Policy

What: Data Policy introduces County defined classification guidelines and standards for all users creating/modifying County Government information. This includes emails, documents, spreadsheets, etc. Data Policy will also implement storage standards and retention policies.

How: Through education, users will become familiar with the classification categories and schema. Using seamless technology built into all products that are used to create, modify, or share information users will be able to quickly and easily classify information.

Why: Data classification is used to protect sensitive information such as patient data, personal information such as SSNs, proprietary information, contract and legal information as well as sensitive information that could be used against the County. Additionally, data classification assists MPIA (FOIA) request by ensuring information is efficiently shared or retained; Data classification also reduces the exposure and liability of the County by introducing retention information that is tagged with each document that is shared, created or modified.

Who: Digital Government, Governance, PMO
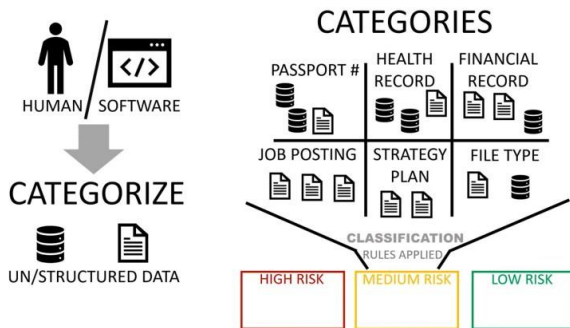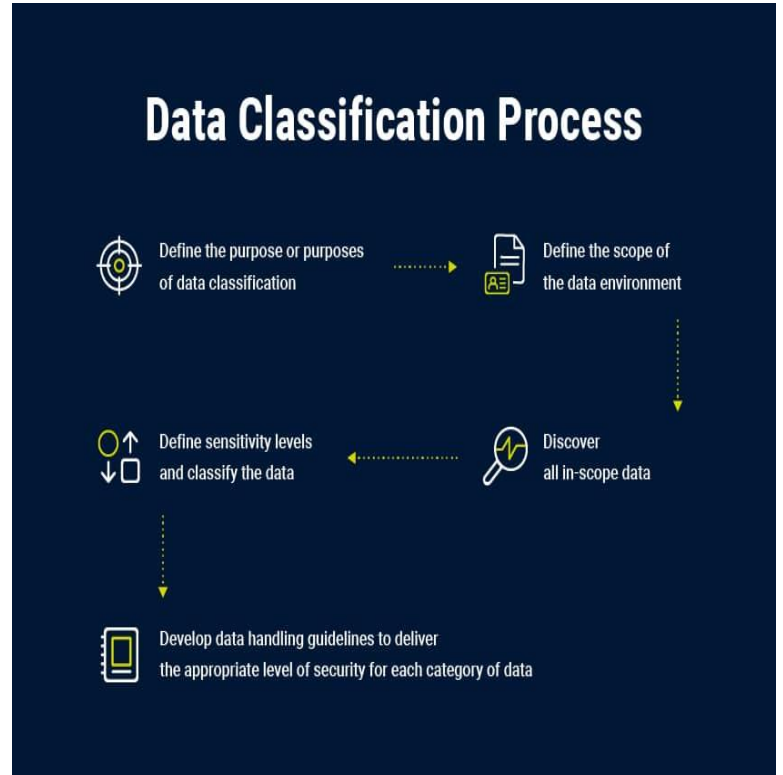
Related Efforts:

1. Innovate Technologies Initiative
2. Cloud Storage Identification and Protection
3. Data segregation
4. Security Group and Active Directory Review & Update
a. Global Address List review & Update
5. Data Portal Legislative Implementation

Business Operations Modernizations:

What: Using technology such as AI, Chatbots, and automation services, many user/customer-facing needs can be automated to reduce user/customer workload and errors on back-end processing by implementation and support teams.

How: Using native resources such as Microsoft Power BI, Microsoft Virtual Assistance OIT can funnel detailed work requirements and customer support needs into automated workflows that review/validate information, then automatically send the request to the next person in the process. Using Organizational Boxes in Outlook workflows can be worked and prioritized by support teams.

Why: Introducing automation reduce customer wait times, introduces efficiency and provides transparency to all stakeholders via an automated dashboard. Algorithms within the automation can provide priority recommendations to support teams based on criticality and take into account work already in the queue. Automated forms will also be able to validate user input reducing errors and coordination time for users and agencies.

Who: Digital Government, EA, Security, PMO, and Leadership

Related Efforts:

1. Innovate Technologies Initiative
2. Process development/refinement, and publishing
3. Data Classification
4. Out of cycle hardware/software requirements
5. OIT internal operating procedures & policies